

IN THE CLAIMS

1. (currently amended) A proxy server, provided between a user terminal and an electronic market server, including a proxy facility for executing authentication and encryption to the electronic market server, instead of the user terminal, in an electronic commercial transaction, comprising:

an establishing means for establishing an encrypted communication session between the user terminal and the proxy server, using public/ and secret keys of the user terminal and an electronic signature both transmitted from the user terminal;

a proxy means for executing authentication of a certificate and exchanging a common key X between the proxy server and the electronic market server, using public/ and secret keys of the electronic market server; and

an informing means for informing the common key X to the user terminal through the encrypted communication session, which common key X is encrypted by using a common key X' that was exchanged between the user terminal and the proxy server;

wherein an encrypted communication is executed directly between the user terminal and the electronic market server by using the common key X that was exchanged between the proxy server and the electronic market server.

2. (previously presented) A proxy server including a proxy facility as claimed in claim 1, further comprising a home card including an encryption managing means for executing the electronic signature and authentication of the certificate in order to execute authentication and exchange of the common key to the electronic market server.

3. (currently amended) A proxy server including a proxy facility as claimed in claim 2, wherein the proxy card includes a logic circuit which enables an access by using a first password input from the user terminal; and a security releasing means for releasing the security for the proxy means by using a second password input from the user terminal, after establishment of the encrypted communication session to the user terminal in which an access was permitted,

4. (previously presented) A proxy server including a proxy facility as claimed in claim 2, wherein the home card comprises an informing means for recording decision information regarding an electronic money in the home card and for informing the recorded decision information to a mail address of the user terminal.

5. (previously presented) A proxy server including a proxy facility as claimed in claim 4, wherein the home card comprises a cancel means for canceling the decision information in the home card based on an authentication information for canceling the decision, and for adding electronic money subtracted by the decision to the electronic money in the home card.

6. (previously presented) A proxy server including a proxy facility as claimed in claim 2, wherein the home card comprises a re-supplement means for supplementing the electronic money by adding supplementary electronic money, which was requested by the user terminal, to the electronic money in the home card, based on the authentication information in an electronic money managing facility provided in the proxy facility.

7. (currently amended) An access card used in an electronic commercial transaction constituted by a user terminal, a proxy server and an electronic market server; the access card being connected to the user terminal; and the proxy server including a proxy facility being provided between the user terminal and the electronic market server for executing authentication and encryption to the electronic market server, instead of the user terminal; the access card comprising:

an establishment means for establishing an encrypted communication session between the user terminal and the proxy server including the proxy facility; and

an encrypted communication means for receiving a common key X, which ~~is was~~ exchanged between the proxy server and the electronic market server after an authentication process for the electronic market server ~~and is encrypted by using a common key X'~~ that was ~~exchanged between the user terminal and the proxy server~~, from the proxy server through the encrypted communication session, and for executing the encrypted communication with the electronic market server directly by using the common key X.

8. (currently amended) A server being able to communicate with a user terminal and the other opposing server having an authentication facility to authenticate the user terminal in accordance with predetermined procedures in an electronic commercial transaction to perform encrypted communication with the user terminal directly, comprising:

a reception unit to receive an identification information and a request for executing an authentication process, from the user terminal;

a decision means for determining whether or not the identification information is stored in an internal or external memory;

a proxy means for executing a part, or all, communication in accordance with the predetermined procedures when the identification information is stored in the memory; and an informing means for informing ~~the a common key X~~ to the user terminal through the encrypted communication session, which common key X is encrypted by using a common key X' that was exchanged between the user terminal and the server.

9. (currently amended) A storage media storing a predetermined program used in a first server being able to communicate with a user terminal and a second server having an authentication facility to authenticate the user terminal in accordance with predetermined procedures in an electronic commercial transaction to perform encrypted communication with the user terminal directly, comprising:

a first step of receiving an identification information and a request for executing an authentication process, from the user terminal;

a second step of determining whether or not the identification information is stored in an internal or external memory;

a third step of executing a part, or all, communication in accordance with the predetermined procedures when the identification information is stored in the memory; and

a fourth step of informing ~~the a common key X~~ to the user terminal through the encrypted communication session, which common key X is encrypted by a using common key X' that was exchanged between the user terminal and the first server.

10. (currently amended) A user terminal being able to communicate with a first server and a second server;

wherein the first server includes a proxy facility for executing authentication with the second server instead of the user terminal, when receiving an identification information and a request for executing an authentication process from the user terminal; and the second server has an authentication facility to authenticate the user terminal in accordance with predetermined procedures and to provide a secret key X for an authorized destination as a result of authentication to perform encrypted communication with the user terminal directly; and

wherein the user terminal comprises a transmitting unit to transmit the identification information used for identifying its own terminal and the request for executing the authentication process, to the first server, and a receiving unit to receive the secret information key X from the first server, which secret key X is encrypted by using a common key X' that was exchanged between the user terminal and the first server.